IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,

Plaintiff and
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

C. A. No. 04-1199 (SLR)

BENCH MEMORANDUM REQUESTING JURY INSTRUCTION RE: PLURALITY OF NETWORK MONITORS

SRI respectfully requests a jury instruction to address a new and unsupported claim construction which has become the centerpiece of Defendants' invalidity case on the hierarchy patents. Defendants' new argument concerns the number of lower-level network monitors that are required by the asserted claims of the '615 and '203 patents. Defendants contend that the claimed "plurality" of network monitors can be met by a single lower-level network monitor in combination with a hierarchical monitor. This contention is inconsistent with the language of the claims themselves, and should be rejected. For the reasons set forth below, SRI respectfully requests the Court instruct the jury that the asserted claims of the '615 and '203 patents require a plurality of network monitors that analyze network traffic data, in addition to one or more hierarchical monitors which receive reports of suspicious activity from the plurality of network monitors.

I. THE PARTIES' DISPUTE

Defendants are now arguing that the use of a single lower-level monitor, plus a hierarchical monitor, meets the "plurality of network monitors" requirement. This argument is driven by the DIDS reference (*see* DDX-1177, attached), which has only a single lower-level LAN monitor reporting to a single higher-level entity called the "DIDS Director."[1] The following questioning of Symantec's expert Mr. Heberlein highlights Defendants' new theory:

> Q: So let's go onto the next limitation: Deploying a plurality of network monitors in the enterprise network.
>
> A: So once again, just looking at the figure, plurality means two or more. So in this particular case, we have two network monitors, or what the courts call network monitors, the lower LAN monitor on the right, and the upper DIDS director, which is also called the network monitor, per the Court's definitions.

Trial Tr. at 1012:16-23 (testimony of Mr. Heberlein). Not only was Mr. Heberlein's expert report silent on this theory – reason enough to reject it – but Symantec has attempted to put the Court's imprimatur on it even though this issue was not joined in the claim construction proceedings. A corrective instruction is therefore necessary, especially because the question of what the claims mean is one of law. It is not appropriate for the parties either to cross examine one another's experts[2] about claim construction or to argue competing claim constructions to the jury. *See O2 Micro Intern. Ltd. v. Beyond Innovation Technology Co., Ltd.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008) ("When the parties present a fundamental dispute regarding the scope of a claim term, it is the court's duty to resolve it."); *CytoLogix Corp. v. Ventana Medical Systems, Inc.*, 424 F.3d 1168, 1172 (Fed. Cir. 2005) ("[B]y agreement the parties also presented expert

[1] The "Host Monitors" depicted in the DIDS reference are not network monitors, because they do not monitor network traffic. Defendants do not rely on the host monitors in making their invalidity argument based on DIDS.

[2] Given when and how Defendants injected this new theory into the trial, however, SRI has no choice but to address it with Mr. Heberlein on cross examination – in addition to seeking the relief sought herein.

witnesses who testified before the jury regarding claim construction, and counsel argued conflicting claim constructions to the jury. This was improper, and the district court should have refused to allow such testimony despite the agreement of the parties."). This Court no doubt intended to avoid just this prospect by properly addressing the disputed claim construction issues well in advance of trial. Indeed, the fact that Defendants are now raising a new claim construction at this late date is reason alone to deny their gambit.

II. THE CLAIMS REQUIRE A PLURALITY OF LOWER-LEVEL MONITORS

The claims are structured to require more than one lower-level monitor. Claim 13 of the '615 patent is representative,[3] and provides:

> An enterprise network monitoring system comprising:
>
> [1] a plurality of network monitors deployed within an enterprise network, **said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data** selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};
>
> [2] **said network monitors generating reports of said suspicious activity**; and
>
> [3] **one or more hierarchical monitors** in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.

'615 Patent, Claim 13 (numbering and emphasis supplied). The structure and terminology of the claims dictate that there be more than one lower-level monitor that analyzes network traffic data. *See Applied Medical Resources Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1333 n.3 (Fed. Cir. 2006) ("It is certainly established that claims are to be construed to preserve the patent's internal coherence.") (citation omitted). Paragraphs [1] and [2] concern the lower-level monitors, which

[3] Asserted independent claim 1 of the '615 patent and asserted independent claims 1 and 12 of the '203 patent are to the same effect.

[1] detect suspicious network behavior and [2] generate reports of said suspicious activity. These paragraphs are unambiguous that the claim requires a plurality of "monitor*s*" doing the detecting and the report generation.

Paragraph [3] concerns the one or more hierarchical monitors, which receive reports from the lower-level network monitors and are distinct from them. While there is no dispute that the hierarchical monitor is itself a type of "network monitor" as construed by the Court – that is, "software and/or hardware that can collect, analyze and/or respond to data" – that does not eliminate the requirement **of the claims** that there must be a plurality of "network monitor*s*" that perform the detecting and report generation functions of paragraphs [1] and [2]. Nor does the Court's claim construction of "hierarchical monitor" (*i.e.*, "a network monitor that receives data from at least one network monitor that is at a lower level in the analysis hierarchy") *ipso facto* allow the **claimed** hierarchy to be made up of a lone lower-level monitor in combination with a lone hierarchical monitor. Defendants can only argue otherwise by focusing on the definitions of "network monitor" and "hierarchical monitor" in isolation, while ignoring what the rest of the claim actually says. In particular, a monitor can only be considered a "hierarchical monitor" if it receives data from at least one network monitor that is at a lower level in the analysis hierarchy -- that is what makes a "hierarchical monitor" "hierarchical." But the one or more hierarchical monitors in the claims must do more, because the claims say so; the claimed hierarchical monitors must receive and integrate reports of suspicious activity generated by a **plurality** of network monitors.

The patentee chose in the claims to use the different terms "network monitor" and "hierarchical monitor" to reflect monitors with different functions (as the specification describes). The patentee used the term "plurality" to modify the "network monitors" of paragraphs [1] and [2]. Regardless of whether the related (but distinct) term "hierarchical monitor" also has the properties of a network monitor and, in isolation, need only receive data from one lower level monitor in order to be considered "hierarchical," it is the patentee's word choice, and in particular the patentee's drafting of the claim as a whole, that controls. *See Board of Regents of the University of Texas System v. BENQ America Corp.*, 533 F.3d 1362, 1371 (Fed. Cir. 2008) ("Different claim terms are presumed to have different meanings.").

The specification consistently describes the "network monitors" by reference to a plurality of network monitors that directly monitor network traffic. *See, e.g.*, '615 patent, at 3:40-50; 6:43-46; 7:43-47; 8:50-56; 9:18-21; 10:14-17; and 12:24-27. Thus, the balance of the intrinsic evidence uniformly confirms that the claims require more than one lower-level network monitor.

SRI submits that the proper construction flows directly from the language of the asserted claims and is readily confirmed by the patent's specification. The Court's claim construction for a single term (hierarchical monitor) requires certain minimum characteristics; the claim then requires more. This is a common occurrence. *See Pause Technology, LLC v. TiVo, Inc.*, 419 F.3d 1326, 1331 (Fed. Cir. 2005) ("However, proper claim construction . . . demands interpretation of the entire claim in context, not a single element in isolation."). Realizing the defects in their prior art, Defendants are attempting to capitalize on a juxtaposition of definitions of particular terms without taking into account the additional requirements which other claim language plainly imposes. Accordingly, SRI respectfully requests that the Court instruct the jury that the asserted claims of the '615 and '203 patents require (1) a plurality of network monitors that analyze network traffic data, in addition to (2) the claimed one or more hierarchical monitors in those claims – that is, a minimum of three monitors, not two, as Defendants have argued.

Dated: September 8, 2008

FISH & RICHARDSON P.C.

By: Thomas L. Halkowski

Thomas L. Halkowski (#4099)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607
halkowski@fr.com

Frank E. Scherkenbach
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

Howard G. Pollack
John N. Farrell
Katherine D. Prescott
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim-Defendant
SRI INTERNATIONAL, INC.

CERTIFICATE OF SERVICE

I hereby certify that on September 8, 2008, I electronically filed with the Clerk of Court the attached BENCH MEMORANDUM REQUESTING JURY INSTRUCTION RE: PLURALITY OF NETWORK MONITORS using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel. In addition, the filing will also be sent via hand delivery:

Richard L. Horwitz
David E. Moore
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899
rhorwitz@potteranderson.com
dmoore@potteranderson.com

Attorneys for
Defendant/Counterclaim Plaintiffs
Internet Security Systems, Inc., a Delaware
corporation, and Internet Security Systems,
Inc., a Georgia corporation

Richard K. Herrmann
Morris James Hitchens & Williams LLP
500 Delaware Avenue, 15th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
rherrmann@morrisjames.com

Attorneys for
Defendant/Counterclaim Plaintiff Symantec
Corporation

I also certify that on September 8, 2008, I electronically mailed the above document(s) to the following non-registered participants:

Paul S. Grewal
Renee DuBord Brown
Day Casebeer Madrid & Batchelder, LLP
20300 Stevens Creek Boulevard, Suite 400
Cupertino, CA 95014
pgrewal@daycasebeer.com
rbrown@daycasebeer.com

Attorneys for
Defendant/Counterclaim Plaintiff Symantec
Corporation

Holmes J. Hawkins, III
Natasha H. Moffitt
King & Spalding LLP
1180 Peachtree Street
Atlanta, GA 30309
hhawkins@kslaw.com
nmoffitt@kslaw.com

Attorneys for
Defendant/Counterclaim Plaintiffs
Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

/s/ Thomas L. Halkowski
Thomas L. Halkowski